Buenas prácticas para la recolección de la evidencia digital en la Argentina

Nicolas Armilla[1], Marisa Panizzi[1], Jorge Eterovic[1], Luis Torres[1].

[1] Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales, Universidad de Morón.
Cabildo 134 – CP (1708) – Morón – Prov. de Bs. As. Tel: 5627-2000
nicolasarmilla@hotmail.com, marisapanizzi@outlook.com, jorge_eterovic@yahoo.com.ar, torreslu@ar.ibm.com

Resumen. En la República Argentina se evidenciaba la ausencia de un manual, un procedimiento o de un código sobre la recolección de la evidencia digital. Esto conllevo a que una gran cantidad de casos quedasen inconclusos y sin resolución, hasta la creación de la Guía de obtención, preservación y tratamiento de evidencia digital de la Procuración General de la Nación Argentina, en Marzo del año 2016. En este trabajo se realiza una revisión sistemática de guías y buenas prácticas de nivel internacional y nacional, identificando los aportes y áreas de vacancias. Se presenta un conjunto de buenas prácticas para la recolección de la evidencia digital en Argentina, logrando subsanar las áreas de vacancia identificadas. Para la correcta validación del conjunto de buenas prácticas, aplicaremos el conjunto a un caso de estudio aplicado a la realidad que consta de la recepción de un mail malicioso en una computadora de escritorio.

Palabras Clave. Informática forense, perito informático, evidencia digital, buenas prácticas, procedimientos en la informática forense.

1 Introducción

Se ha realizado una investigación exploratoria documental respecto a definiciones de informática forense, antecedentes actuales en el ámbito internacional y nacional.

Darahuge define la Informática Forense como el conjunto muldisciplinario de teorías, técnicas y métodos de análisis, que brindan soporte conceptual procedimental a la investigación de la prueba indiciaria informática [1][2].

Kovacich define la Informática Forense como la aplicación legal de métodos, protocolos y técnicas para obtener, analizar y preservar evidencia digital relevante a una situación en investigación [3].

Gómez define la Informática Forense como aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. O también lo define como una ciencia que busca reproducir científicamente con una metodología estricta de los hechos acontecidos y su correlación para determinar el grado de impacto, y posteriormente establecer en coordinación con otros entes intervinientes, mecanismos tendientes a evitar nuevamente su ocurrencia, que van desde el marco normativo hasta la utilización de mecanismos técnicos [4].

Listek en el Diario La Nación plantea que el Gobierno quiere normas claras para obtener pruebas digitales en los procesos judiciales [5].

La Procuración General de la Nación menciona que uno de los temas que puede tocarse desde ahora es el relativo a la evidencia digital, ya que su adecuada obtención, conservación y tratamiento es un elemento clave, entre muchos otros, para asegurar el éxito de las investigaciones [6].

Luego de revisar los antecedentes en nuestro país, nos planteamos como problema de esta investigación la escasa maduración de procedimientos para la recolección de la evidencia digital en la informática forense en la República Argentina.

En los últimos años los peritos informáticos se basaron en procedimientos y buenas prácticas de otros países tales como Canadá, Estados Unidos, Reino Unido y Hong Kong. En la actualidad, a partir del año 2016 se cuenta con la nueva resolución de la Procuración General de la Nación [6].

Utilizando el método de revisiones sistemáticas de Argimón [7] se ha realizado una investigación documental sobre los procedimientos y buenas prácticas que se detallan a continuación:

- Guía de buenas prácticas para evidencia digital. [8].
- Computación Forense - Parte 2: Mejores Prácticas. [9].
- Guía para recolectar y archivar evidencia - RFC 3227. [10].
- Investigación en la escena del crimen electrónico. [11].
- Guía de obtención, preservación y tratamiento de evidencia digital. [6].

Se ha detectado que el inconveniente de basarse en procedimientos y buenas prácticas de otros países presenta diferencia de factores tecnológicos, sociales, culturales y legales respecto a los de nuestro país.

En este contexto, este artículo presenta las guías y buenas prácticas consideradas para el análisis comparativo (Sección 2), se presenta el conjunto de buenas prácticas para la recolección de la evidencia digital (Sección 3), se presenta un caso de estudio para la validación de la propuesta de solución (Sección 4) y se formulan conclusiones y futuras líneas de trabajo (Sección 5).

2 Guías y Buenas Prácticas consideradas

En esta sección se presentan las guías y buenas prácticas que se han contemplado para el estudio comparativo, la Guía de buenas prácticas para evidencia digital [8]

(sección 2.1), Computación Forense - Parte 2: Mejores Prácticas. [9] (sección 2.2), Guía para recolectar y archivar evidencia - RFC 3227. [10] (sección 2.3), Investigación en la escena del crimen electrónico [11] (sección 2.4) y Guía de obtención, preservación y tratamiento de evidencia digital. [6] (sección 2.5). Por último, se presenta el resultado del análisis realizado (sección 2.6).

2.1 Guía de buenas prácticas para evidencia digital.

La Asociación de Jefes de Policía (ACPO – Association of chief police officers) del Reino Unido mediante su departamento de crimen basado en informática, publicó esta guía en el año 2012 [8].

El propósito de este documento no es solo proveer una guía para asistir a la ley sino asistir a la investigación de la seguridad informática e informática forense tanto en escenas de crímenes como incidentes [8].

Es necesario aclarar que esta guía no pretende ser una receta desde A-Z de la forensia digital, o un manual de instrucciones específico que indique como realizar todas las tareas. Debe abarcar un cuadro general y proporciona una estructura subyacente a lo que se requiere en las Unidades Forenses Digitales [8].

2.2 Computación Forense - Parte 2: Mejores Prácticas

El ISFS, Information Security and Forensic Society (Sociedad de Seguridad Informática y Forense) creada en Hong Kong, publicó "Computación Forense - Parte 2: Mejores Prácticas" (Computer Forensics – Part 2: Best Practices). Esta guía cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la escena del crimen hasta la presentación de los reportes en la corte. Su estructura es:

a) Introducción a la computación forense.
b) Calidad en la computación forense.
c) Evidencia digital.
d) Recolección de Evidencia.
e) Consideraciones legales (orientado a la legislación de Hong Kong).
f) Anexos [9].

2.3 Guía para recolectar y archivar evidencia

El propósito de esta guía es proveer a los peritos un sistema de pautas sobre la recolección y archivo de evidencias digitales, para un incidente de seguridad determinado [10].

No hace falta insistir en que todos los peritos del sistema estrictamente deben seguir estas pautas cada vez que tienen un incidente de seguridad, lo importante es proveer una guía sobre que deberíamos hacer si ellos eligen recolectar y proteger la informaron relacionada con un intruso [10].

Dicha recolección representa un esfuerzo considerable por parte del perito. En los últimos años se han realizado grandes progresos para acelerar la reinstalación del Sistema Operativo y facilitar la reversión de un sistema a un estado "conocido" haciendo de este modo, la "opción fácil" aún más atractiva. Mientras tanto, poco se ha realizado para suministrar formas fáciles para archivar la evidencia (la opción difícil).

Además las capacidades de memoria y de disco en aumento y el uso más difundido de cautela y de tácticas de cubrir huellas por parte de los atacantes han exacerbado el problema [10].

Si la recolección de evidencia se realiza correctamente, es mucho más útil para aprehender al atacante y representa una oportunidad mucho mayor en ser admitida como hecho en un juicio [10].

Se deberían utilizar estas pautas como una base para formular los procedimientos de recolección de evidencia de sitio y se deberían incorporar los procedimientos de sitio en una documentación de manejo de incidente [10].

Una vez que se hayan formulado los procedimientos de recolección de evidencia de sitio, deberían tener la aplicación de la ley para tu jurisdicción confirmando que son adecuados [10].

2.4 Investigación en la escena del crimen electrónico

La investigación en la escena del crimen electrónico fue creada por el Departamento de Justicia de los Estados Unidos de América en 2001 [11].

Dentro de las principales responsabilidades se encuentran la de preservar la escena crimen electrónico, recolectar y resguardar la evidencia digital [11].

Se ocupa de las situaciones encontradas en la escena del crimen y evidencia electrónica digital [11].

Tratándose de pruebas digitales, los principios forenses y procesales generales se deberían aplicar en:

- El proceso de recolección, aseguramiento y transporte de pruebas digitales, las mismas no debieran cambiar.
- Las pruebas digitales sólo deberían ser examinadas por los entrenados expresamente con ese objetivo.
- Todo lo hecho durante el transporte y el almacenaje de pruebas digitales se debería documentar, conservarse y encontrarse disponibles para la revisión [11].

2.5 Guía de obtención, preservación y tratamiento de evidencia digital

La obtención, conversación y tratamiento de la evidencia digital es un elemento clave, entre muchos otros, para asegurar el éxito de las investigaciones, eje central de preocupación de la comunidad internacional para la investigación transfronteriza eficaz de estos delitos [6].

No pretende abarcar la totalidad de procedimientos a tener en cuenta, ni ahondar en cuestiones técnicas reservadas a los expertos en seguridad y en informática, sino

brindar recomendaciones utilizadas a nivel mundial para incautar, analizar y preservar evidencia digital que deben ser tenidas en cuenta por los operadores judiciales [6].

2.6 Dimensiones consideradas para el análisis

En esta sección se plantean las dimensiones que se han considerado para el análisis de las buenas prácticas y procedimientos a nivel nacional como internacional Las dimensiones consideradas son:

- Evaluación de escena: El perito informático debe tomar medidas para garantizar la seguridad de todas las personas en el lugar de los hechos y para proteger la integridad de todas las pruebas, tanto tradicionales como electrónicas [11].
- Herramientas y equipamientos: Generalmente, y dependiendo del problema a analizar, se sugiere aplicar una combinación de herramientas, para asegurar la efectividad que se debe tener en estos casos donde la libertad de las personas puede estar comprometida, y ello podría depender del resultado de una pericia informática aplicando herramientas de forensia. [12].
- Dispositivos electrónicos: La mayoría de los dispositivos electrónicos referidos a informática forense se aplica a computadoras y dispositivos digitales en general. Pero también existen otros dispositivos que requieren consideraciones adicionales [9].
- Recolección: La recolección de la evidencia digital, como cualquier otra evidencia, debe manejarse cuidadosamente y de una manera que preserve su valor probatorio. Esto se refiere no sólo a la integridad física de un artículo o dispositivo, sino también a los datos electrónicos que contiene. Por lo tanto, ciertos tipos de pruebas informáticas requieren una recolección especial [11].
- Almacenamiento y transporte: Las acciones no deben agregar, modificar o destruir datos almacenados en una computadora u otros medios. Las computadoras son instrumentos electrónicos frágiles que son sensibles a la temperatura, humedad, choque físico, electricidad estática y fuentes magnéticas. Por lo tanto, se deben tomar precauciones especiales al empaquetar, transportar y almacenar evidencia electrónica [11].
- Análisis: El análisis forense digital se corresponde con un conjunto de técnicas destinadas a extraer información valiosa de dispositivos, sin alterar el estado de los mismos. Esto permite buscar datos que son conocidos previamente, tratando de encontrar un patrón o comportamiento determinado, o descubrir información que se encontraba oculta [1][2].
- Reporte: Los reportes son información escrita con una terminología determinada, haciendo referencia a los detalles específicos de un caso particular [9].

En la Tabla 1, se presenta el grado de cumplimiento de las dimensiones de análisis consideradas para análisis de las buenas prácticas y procedimientos a nivel nacional e internacional.

Tabla 1. Tabla Comparativa de buenas prácticas y procedimientos a nivel internacional y nacional

	Internacional				Nacional
	Guía de buenas prácticas para la evidencia digital (ACPO, 2012)	Computación Forense - Parte 2: Mejores Prácticas (ISFS, 2009)	Guía para recolectar y archivar evidencia – RFC3227 (RFC, 2002)	Investigación en la escena del crimen electrónico (NIJ, 2001)	Guia de obtención, preservación y tratamiento de evidencia digital (Procuración General de la Nación, 2016)
Evaluación de Escena		■		■	■
Herramientas y equipamientos		■	■	■	■
Dispositivos electrónicos				■	■
Recolección	■	■	■	■	■
Almacenamiento y transporte	■	■	■	■	■
Análisis	■				■
Reporte	■	■			

Los resultados de análisis a los cuales se ha arribado con la Tabla Comparativa de (Tabla 1.) permiten formular las siguientes conclusiones: ninguna de las guías y buenas prácticas analizadas custodian las dimensiones analizadas en su totalidad.

A partir de este análisis y de la identificación de las áreas de vacancias detectadas, se propone un conjunto de buenas prácticas para la recolección de la evidencia digital que considere todas las dimensiones analizadas (sección 3).

3 Propuesta del conjunto de buenas prácticas para la recolección de la evidencia digital en Argentina

El conjunto de buenas prácticas propuesto se denominará "Conjunto de Buenas Prácticas para la Recolección de la Evidencia Digital, cuya abreviatura será Co. Bu. P.R.E.D.A.

Este conjunto de buenas prácticas se compone de siete (7) etapas, en este contexto cada una de las etapas equivale a la dimensión de análisis planteada en la Tabla 1:

1. Evaluación de escena
2. Herramientas y equipamientos
3. Dispositivos electrónicos
4. Recolección
5. Almacenamiento y transporte

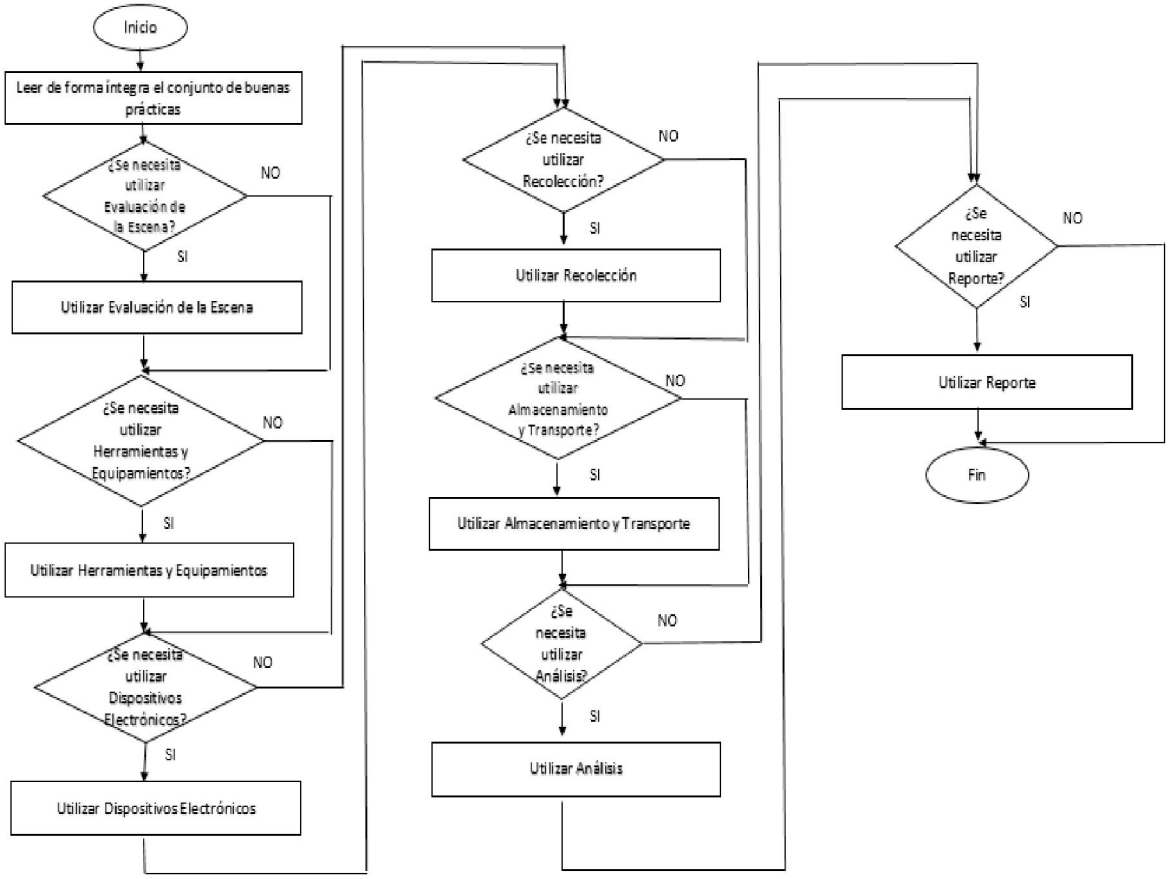
6. Análisis
7. Reporte

Cada etapa propone prácticas y herramientas, las prácticas hacen referencia a las actividades que tiene que realizar el perito en cada etapa y las herramientas refieren a los conocimientos, softwares y artefactos que necesitan para poder llevar a cabo las prácticas en cada etapa. Es importante aclarar que este conjunto de buenas prácticas contempla los factores tecnológicos, legales, sociales y culturales en Argentina.

Este conjunto de buenas prácticas está dirigido a los peritos con el propósito de facilitarles su tarea de recolección de la evidencia digital. Este conjunto puede ser utilizado en su totalidad o ajustándolo a la necesidad de cada uno de los escenarios planteados. Es recomendable que antes de utilizar un conjunto de buenas prácticas sea leído en su totalidad para comprender cuáles son los puntos que se adaptan al caso en particular y cuales no para luego aplicarlos de forma óptima.

En la Figura 1 se presenta un diagrama de flujo, el cual sintetiza la manera de utilización del conjunto de buenas prácticas propuesto.

Figura 2. Diagrama de flujo para utilizar Co. Bu. P.R.E.D.A



4 Caso de estudio para la validación de la propuesta

El caso de estudio seleccionado para validar la propuesta del conjunto de buenas prácticas consiste en la recepción de un mail con una supuesta amenaza que recibe un usuario final en una computadora de escritorio con sistema operativo Windows 10, la cual se encuentra conectada a la energía eléctrica.

La selección de este caso se debe a que es un problema común en el ámbito de la informática forense.

En la Tabla 2, se presenta la aplicación del Conjunto de Buenas Prácticas para la Recolección de la Evidencia Digital en la Argentina (Co. Bu. P.R.E.D.A.) para analizar la supuesta amenaza de un mail malicioso dentro de la computadora de escritorio.

De la aplicación de Co. Bu. P.R.E.D.A. en el caso de estudio (Tabla 2.) se arribó a la conclusión que ha sido necesario considerar las siete (7) etapas del conjunto de buenas prácticas junto con sus prácticas y herramientas.

5 Conclusiones y futuras líneas de trabajo

Se ha presentado una revisión sistemática de guías y buenas prácticas de recolección de evidencia digital que ha permitido identificar las vacancias de los procedimientos existentes.

Se ha logrado la construcción de un conjunto de buenas prácticas compuesta por siete (7) etapas contemplando prácticas y herramientas que se adaptan a los factores tecnológicos, sociales y culturales de Argentina.

Se ha logrado validar el conjunto de buenas prácticas en un caso de estudio.

Como futuras líneas de trabajo se identifican:

- La experimentación del Conjunto de Buenas Prácticas para la Recolección de la Evidencia Digital en Argentina (Co. Bu. P.R.E.D.A.) en casos relacionados a fraudes de telecomunicaciones, violencia doméstica, investigaciones referidas a estupefacientes, amenazas y/o acoso vía correo electrónico, homicidios, copia ilegal de software, abuso infantil y pornografía.
- Se evidencia un área de vacancia en las copias bit a bit del Sistema Operativo en dispositivos móviles (Android, IOS, Windows phone) y manuales de recolección de evidencia digital para los mismos.

Tabla 2. Aplicación de Co. Bu. P.R.E.D.A. en caso de estudio.

Etapas	Prácticas	Herramientas
Evaluación de la escena	-Preservación de la computadora -Aislar la computadora de personas ajenas a la investigación	-Cámara de fotos. -Cinta del lugar del crimen. -Guantes.
Herramientas y equipamientos	-Actualización sobre herramientas y equipamientos relacionados con la informática forense.	- Cámara de foto, cinta del lugar del crimen, guantes, instrumentos no magnéticos, bloc de notas, cajas de cartón, registros, etiquetas, marcador y bolso antiestático. -Conocimiento sobre Windows 10, hardware, periféricos, redes y seguridad informática. -Programas para hacer copia bit a bit, para examinar estado del sistema y para generar imágenes.
Dispositivos electrónicos	-Evitar perdida de información volátil. -Interés principal por Windows 10, mails, historial de internet y logs.	-Conocimiento sobre Windows 10. -Conocimiento sobre hardware. -Conocimiento sobre periféricos.
Recolección	-Etiquetar, documentar, marcar, fotografiar, filmar y rotular la computadora. -Individualizar todos los cables de la computadora. -Verificar registro para ver si se eliminó algún dato.	-Guantes. -Instrumentos no magnéticos.
Almacenamiento y transporte	-Procedimiento de embalaje de computadora. -Procedimiento de transporte de computadora. -Procedimiento de almacenaje de computadora. -Cadena de la custodia.	-Bloc de notas. -Cajas de cartón. -Guantes. -Registros del inventario de pruebas. -Etiquetas adhesivas de pruebas. -Bolso antiestático. -Marcador permanente.
Análisis	-Copia bit a bit del sistema operativo Windows 10. -Estrategia forense (concentrarse en los mails maliciosos). -Situar datos en listado de la evidencia digital.	-Conocimiento en Windows 10. -Programas para examinar procesos. -Programas para examinar el estado del sistema. -Programa para hacer copias bit a bit. -Programas para generar imágenes esenciales y para poder examinarlas.
Reporte	-Generación de reporte técnico. -Conclusiones alcanzadas.	-Conocimiento en Windows 10. -Conocimiento en seguridad informática. -Conocimiento en redes.

Referencias

1. Darahuge Maria Elena – Arellano González Luis Enrique, Manual de informática forense 1, Buenos Aires, 2011.
2. Darahuge Maria Elena – Arellano González Luis Enrique, Manual de informática forense 2, Buenos Aires, 2012.
3. Kovacich Gerald, High-Technology Crime Investigator's Handbook: Working in the Global Information Environment, United States of America, 2000.
4. Gómez Luis A., La informática forense: una herramienta para combatir la ciberdelincuencia, Buenos Aires, 2012.
5. Listek Vanesa, El gobierno quiere normas claras para obtener pruebas digitales en los procesos judiciales, Diario La Nacion - Argentina, viernes 19 de agosto de 2016. http://www.lanacion.com.ar/1929918-EL-GOBIERNO-QUIERE-NORMAS-CLARAS-PARA-OBTENER-PRUEBAS-DIGITALES-EN-LOS-PROCESOS-JUDICIALES
6. Procuración General de la Nación, Guía de obtención, preservación y tratamiento de evidencia digital, publicada en la Resolución PGN-0756-2016-001, 31 de marzo de 2016.
7. Argimón J. 2004. Métodos de Investigación Clínica y Epidemiológica. Elsevier España, S.A. ISBN 9788481747096.
8. ACPO: Association of Chief Police Officers, Good Practice Guide for Digital Evidence, Reino Unido, 2012.
9. ISFS: Information Security and Forensic Society, Computación Forense – Parte 2: Mejores Prácticas, Hong Kong, 2009.
10. RFC: Request for Comments, RFC 3227: Guía para recolectar y archivar evidencia, 2002.
11. NIJ: National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders - Second Edition, Washington, 2001.
12. Piccirilli Dario, La forensia como herramienta en la pericia informática, Buenos Aires, 2013.
13. Piccirilli Dario. PROTOCOLOS A APLICAR EN LA FORENSIA INFORMÁTICA EN EL MARCO DE LAS NUEVAS TECNOLOGÍAS (PERICIA – FORENSIA y CIBERCRIMEN), La Plata – Prov. Buenos Aires, 2015.
14. ENFSI: European Network of Forensic Science Iinstitues, GUIDELINES FOR BEST PRACTICE IN THE FORENSIC EXAMINATION OF DIGITAL TECHNOLOGY, Europa, 2009.
15. Acurio Del Pino Santiago, Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0, Ecuador, 2009.
16. Darahuge Maria Elena – Arellano González Luis Enrique, La cadena de custodia informaticó forense, Buenos Aires, 2016.
17. Darahuge Maria Elena – Arellano González Luis Enrique, Aplicaciones Creativas e Innovadoras en Informática. Desarrollos informáticos creativos e innovadores, Buenos Aires, 2016.